

Clerk of Court  
U.S. Bankruptcy Court, District of Delaware  
824 N. Market Street, 3rd Floor  
Wilmington, DE 19801

RECEIVED

2025 NOV 20 A 10:30

**Re: In re FTX Trading Ltd., et al., Case No. 22-11068 (JTD) — Jointly Administered**  
**(Chapter 11)**  
**Filing by Daizhuo Chen (pro se)**

CLERK  
US BANKRUPTCY COURT  
DISTRICT OF DELAWARE

Dear Clerk:

Enclosed please find the

- Reply in Further Support of Motion for Late KYC Completion; and
- the accompanying Certificate of Service,

in the above-referenced case, submitted for filing on the docket.

Thank you for your assistance.

Dated: November 18, 2025

/s/ Daizhuo Chen

Daizhuo Chen (pro se)  
1726 Maddux Dr  
Redwood City, CA 94061  
Phone: 646-286-8876  
Email: chendaizhuo@gmail.com

UNITED STATES BANKRUPTCY COURT  
DISTRICT OF DELAWARE

In re:  
FTX TRADING LTD., et al., Debtors.  
Chapter 11  
Case No. 22-11068 (JTD)  
(Jointly Administered)

**REPLY IN FURTHER SUPPORT OF MOTION FOR LATE KYC  
COMPLETION**

I submit this reply in further support of my Motion for Entry of an Order Authorizing Late Completion of Customer KYC [D.I. 33349] (the "Motion").

**I. INTRODUCTION**

The Trust's objection<sup>1</sup> tries to tell a simple story: I supposedly ignored "multiple official emails" for years and had a "self-created predicament" by failing to follow clear instructions. That is not what happened. The Debtors told customers to treat @kroll.com, and later @ftx.com, as the safe domains, while repeatedly routing essential KYC emails through no-reply@sumsub.com and in.sumsub.com with no clear, in-email explanation of why that third-party domain should be trusted. Following the Debtors' own security guidance pointed away from, not toward, the channel the Trust now calls "authorized" and "official."

I am a single retail customer with a scheduled claim. The Debtors and the FTX Creditors' Liquidating Trust (together, the "Trust") do not dispute my scheduled balance or the underlying validity of my claim. The only issue is that I did not complete the Know Your Customer ("KYC") process by the applicable deadlines. I am not asking the Court to overturn the KYC

---

<sup>1</sup> Objection of The FTX Recovery Trust To Motion for Entry of An Order Authorizing Late Completion of Customer KYC. Ref No 33575.

regime, reopen the bar date, or alter the plan. I am asking for narrow, individualized relief: that my previously accepted, scheduled claim be restored for the limited purpose of allowing me to complete KYC now so that it can be paid under the existing framework.

This is not a case where a creditor ignored clear, consistent instructions. I followed an official Kroll reminder into the `claims.ftx.com` portal, accepted my scheduled claim, and received an “Acceptance of Scheduled Claim” email that said nothing about incomplete KYC and instead told me that all Kroll emails would come from `@kroll.com` and should be treated as trusted. Later, in February 2025, FTX Support told customers to “validate the sender’s domain is `@ftx.com` before proceeding.” The KYC prompts I actually received matched neither rule: they came from `no-reply@sumsub.com` and routed to `in.sumsub.com`, with no clear, in-email explanation of who Sumsub was or why that domain was safe for my identification documents. In that environment, I made a mistake in not confirming my status sooner. My delay was the product of mixed fault—my own failure to seek clarification, combined with confusing and fragmented communications—not casual indifference.

Under Bankruptcy Code § 502(j), Federal Rule of Civil Procedure 60(b), and Bankruptcy Rule 9006(b)(1), I respectfully submit that this record falls within the kind of confusing, mixed-fault circumstances courts have treated as “excusable neglect,” and that granting limited, KYC-only relief as to my claim would not prejudice the estate.

## **II. FACTUAL BACKGROUND**

### **A. Scheduling and Acceptance of My Claim**

My claim was scheduled by the Debtors based on their own books and records. I did not contest the amount. On or about September 22–23, 2023, I logged in to the official `claims.ftx.com` portal and accepted my scheduled claim.

I do not recall every screen or every click from nearly two years ago. However, the Trust's general description—that their vendor's records show I accessed a verification flow, provided certain information (such as address, selfie, or questionnaire responses), and did not upload a valid identification document—is generally consistent with my recollection that I went through a verification process after logging into the `claims.ftx.com` portal. At the time, I understood this as part of the FTX/Kroll portal process, not as initiating a separate relationship with a third-party vendor. I do not clearly recall whether I completed that final step, and to the extent contemporaneous records indicate that an identification document was not uploaded, I defer to those records.

### **B. September 22–23, 2023: Portal Login, Claim Acceptance, and KYC Initiation**

To the best of my recollection, on September 22, 2023 I received an email titled “In re FTX Trading Ltd. – Customer Claims Bar Date Reminder” from `ftx@noticing.ra.kroll.com` (Exhibit G) and used that official message to log in to `claims.ftx.com`. On September 23, 2023, I accepted my scheduled claim through the `claims.ftx.com` portal.



I understand that the Trust's records<sup>2</sup> reflect that I accessed the vendor portal (in.sumsub.com) that same day and proceeded through some steps but did not upload an identification document. That is consistent with the verification flow being linked from within the claims.ftx.com portal, rather than from a stand-alone in.sumsub.com email.

Crucially, after that session, I received an "Acceptance of Scheduled Claim" email dated September 23, 2023 from noreply.efiling@ra.kroll.com (previously filed as Exhibit

A). That email:

- Confirms that my scheduled claim had been accepted;
- Does not state that KYC was incomplete; and
- Includes the statement that "all emails sent by Kroll Restructuring Administration LLC will now have the domain @kroll.com," and recommends that recipients update their email permissions accordingly.

I did not receive any contemporaneous notice that verification remained incomplete following that portal session. Having just followed an official Kroll reminder into the claims.ftx.com portal, completed the acceptance process, and then received an acceptance email with no KYC warning and specific @kroll.com domain guidance, I reasonably believed at that time that I had done what was required.

That combination—(1) portal-based initiation, (2) an "Acceptance of Scheduled Claim" email that is silent about incomplete KYC, and (3) explicit @kroll.com domain guidance—made later prompts from non-@ftx.com, non-@kroll.com senders (e.g.,

---

<sup>2</sup> Trust Objection, Paragraph 3.

no-reply@sumsub.com routing to in.sumsub.com) appear suspicious rather than authoritative.

I am not aware of any communication in the days immediately following that session (around September 23–30, 2023) stating that my verification remained incomplete. If such documents exist, I will defer to them; my recollection is as stated.

**C. Repetitive Third-Party KYC Prompts and Increasing Suspicion (Late 2023–2024)**

Between November 2023 and August 2024, I received multiple KYC prompts from no-reply@sumsub.com that referenced the FTX portal but directed me to in.sumsub.com, a third-party domain. These emails include messages dated November 1, 2023; March 1, 2024; April 9, 2024; May 7, 2024; and August 19, 2024 (previously filed as Declaration Exhibits D-2 through D-6).

These prompts:

- Displayed “FTX” as the sender name, used FTX branding (including the logo), and ended with “Best regards, Customer Support Team,” without mentioning Sumsub at all, even though the actual sender address was no-reply@sumsub.com (a non-@ftx.com domain);
- Came from a non-@kroll.com sender, despite the earlier acceptance email highlighting @kroll.com as the Kroll domain;
- Linked to in.sumsub.com, which is not obviously associated with FTX or the Debtors;

- Did not contain a simple, in-email explanation of who Sumsb was or why that domain should be trusted with my identification document;
- Stated in the body that “you will need to upload all requested documents as indicated on the KYC section of the customer claims portal (claims.ftx.com),” but in those emails the “claims.ftx.com” text itself was not clickable (unlike prior Kroll emails); the only actionable link was a “Verify me” button that led directly to `in.sumsb.com`;
- Stated that “our customer support team is ready to assist you,” but did not identify whether that referred to FTX, Kroll, or a third-party vendor, and provided no contact information. Combined with the “no-reply” sender address, this made it unclear how a cautious user was supposed to verify the legitimacy of the request; and
- Asked me to upload highly sensitive identification documents—“a valid and unexpired ID, such as a passport, national ID card, or driver’s license depending on country of issuance selected”—through that unfamiliar third-party flow.

As is commonly emphasized in phishing-prevention guidance, visual elements such as the sender name, branding, and email body can be easily imitated, so cautious users often pay particular attention to the actual email address and domain. In these KYC prompts, the visible branding and text referenced FTX and the claims.ftx.com portal, but the underlying sender domain was `no-reply@sumsb.com` and the only actionable link directed me to `in.sumsb.com`, not to `@ftx.com` or `@kroll.com`. During a time when crypto-related phishing and identity theft were widely reported, repeated prompts from an unfamiliar third-party domain asking for highly sensitive identification information, and not matching the domains (`@ftx.com`, `@kroll.com`) I had been told to rely on, shared characteristics often associated with phishing, especially given



my belief—after the claims.ftx.com portal session and acceptance email—that I had already completed the required steps through official channels.

The Trust cites an “Official Email Addresses” webpage<sup>3</sup> listing no-reply@sumsub.com as a legitimate sender. However, that information was static and passive; it was not clearly pushed into the Sumsub email content itself. The earlier KYC prompts did not contain an in-email explanation of the vendor relationship or how to reconcile the domain mismatch.

According to the Trust, that webpage was “posted at least as of December 2024”; I cannot independently verify the posting date. In any event, a December 2024 webpage—well after my September 23, 2023 portal session and acceptance email—does not cure or retroactively resolve the earlier confusion.

**D. Later Security Guidance: “Validate the Sender’s Domain is @ftx.com”**

On February 9, 2025—after the Court entered the KYC Objection Order on February 3, 2025 (setting a March 1 “commence” date and a June 1 “complete” date)—FTX Support (support@ftx.com) sent an email that prominently displayed at the top: “Please validate the sender’s domain is @ftx.com before proceeding.” (Exhibit H.) This was presented as an explicit phishing-prevention rule.

My KYC prompts, by contrast, arrived from non-@ftx.com addresses and routed to in.sumsub.com, without a clear, in-email explanation of why that vendor domain should be trusted with identification information. Following the later “validate @ftx.com” security rule

---

<sup>3</sup> Trust Objection, Paragraph 22.



would lead a cautious user to distrust the very Sumsb emails that the Trust now characterizes as “authorized”.

When combined with the earlier @kroll.com guidance in my September 23, 2023 acceptance email, this created a clear tension between the security advice I was given (trust @ftx.com and @kroll.com) and the actual implementation of KYC (non-@ftx.com, non-@kroll.com Sumsb emails directing to in.sumsb.com).

#### **E. My Delay and Subsequent Actions**

In the months following my September 23, 2023 portal session and acceptance email, I did not contact the claims agent or support to expressly confirm whether my KYC was complete. That failure to verify, in the face of ambiguous and conflicting signals, is the neglect I am asking the Court to excuse.

Once I understood that non-completion of KYC would result in a complete loss of my otherwise accepted scheduled claim, I acted promptly to seek information and relief. I have at all times acted in good faith, and have never attempted to increase my claim size, dispute the scheduled amount, or gain any strategic advantage.

### **III. LEGAL STANDARD**

Section 502(j) of the Bankruptcy Code authorizes the Court to reconsider a claim that has been allowed or disallowed “for cause” and to “allow or disallow such claim according to the equities of the case.”

Where a claim has effectively been disallowed or expunged due to a missed procedural step (here, KYC completion), courts apply Federal Rule of Civil Procedure 60(b), as incorporated by Bankruptcy Rule 9024, and the “excusable neglect” framework set forth in *Pioneer Investment Services Co. v. Brunswick Associates Limited Partnership*, 507 U.S. 380 (1993).

Separately, Bankruptcy Rule 9006(b)(1) provides that, after a deadline has passed, the court may enlarge the time “where the failure to act was the result of excusable neglect.”

Under *Pioneer*, excusable neglect is evaluated by considering:

- The danger of prejudice to the debtor or estate;
- The length of the delay and its potential impact on judicial proceedings;
- The reason for the delay, including whether it was within the reasonable control of the movant; and
- Whether the movant acted in good faith.

The standard does not require that the creditor have acted perfectly. It contemplates circumstances in which a party makes a mistake in a confusing or difficult environment, and the court exercises equitable discretion to grant relief where the overall equities warrant it.

#### **IV. APPLICATION OF THE PIONEER FACTORS**

##### **A. Prejudice to the Estate**

Granting narrow relief in my case would not meaningfully prejudice the Debtors, the Trust, or other creditors.

- I am a single, scheduled retail claimant.

- The amount of my scheduled claim is modest relative to the overall size of the estate.
- I am not seeking to reopen the bar date, relitigate the plan, or disturb final distributions; I am asking only to be allowed to complete KYC so that my previously scheduled claim can be paid in the ordinary course.

Processing one additional KYC verification and including one additional scheduled claim in the distribution pool is, at most, a de minimis administrative burden. The Trust's floodgates concern can be addressed by making clear that any relief is limited to the specific facts of my situation.

The Trust also acknowledges that, where customers "experienced technical difficulties ... and contacted the FTX Recovery Trust prior to the deadline, the FTX Recovery Trust has reasonably worked with such customers to resolve those issues."<sup>4</sup> Processing one additional verification now, on a fact-specific, non-precedential basis, is operationally trivial and does not disturb distributions.

#### **B. Length of Delay and Impact on Proceedings**

The relevant delay is the period between when I could and should have completed KYC and when I sought relief.

Once I understood that the KYC non-completion had the effect of expunging my otherwise accepted scheduled claim, I moved promptly. Any incremental delay attributable to my motion and this reply is short in the context of these chapter 11 cases and has minimal impact on the broader administration of the estate.

---

<sup>4</sup> Trust Objection, Paragraph 10.

A limited order that restores my claim solely for the purpose of completing KYC would not require re-opening the claims reconciliation process or re-designing distributions. Its impact on the proceedings would be negligible.

### **C. Reason for the Delay**

The Trust characterizes my situation as a “self-created predicament”<sup>5</sup> arising from my failure to respond to “clear” instructions. That description omits critical facts and oversimplifies what actually happened.

#### *1. Fragmented and conflicting communications*

The KYC design and messaging had several features that made confusion and drop-off foreseeable among cautious users:

- Third-party domain without in-email explanation. KYC notices arrived from `no-reply@sumsub.com` and directed me to `in.sumsub.com`, a third-party domain not obviously associated with FTX, without a plain, in-email explanation of who Sumsub was or why that domain should be trusted with my identification document.
- Passive “official addresses” listing. The Trust later published an “Official Email Addresses” page that listed `no-reply@sumsub.com`, but that information was static. It was not embedded in, or prominently surfaced within, the emails that were asking for sensitive documents.
- Domain guidance that conflicted with the KYC channel. My September 23, 2023 “Acceptance of Scheduled Claim” email told me that all Kroll emails would come from

---

<sup>5</sup> Trust Objection, Paragraph 2.



@kroll.com and recommended that I treat that as the trusted domain. Later, on February 9, 2025, FTX communications instructed customers to “validate the sender’s domain is @ftx.com before proceeding.” The Sumsb prompts matched neither @ftx.com nor @kroll.com, and did not clearly explain the exception. This created a direct tension between the security guidance and the KYC implementation.

## *2. Portal-based initiation and reasonable belief of completion*

The Trust’s vendor logs show that on or about September 23, 2023 I accessed the Sumsb KYC portal, completed certain steps, and did not upload an identification document, so the system marked my KYC as incomplete. I do not have a precise memory of each screen or how I reached that site. I searched my email for messages from Sumsb (including no-reply@sumsub.com) dated around September 22–23, 2023 and found none; the earliest Sumsb email in my inbox is from November 1, 2023 (previously filed Exhibit D-2). Combined with my recollection of accessing the claims.ftx.com portal through the Kroll bar-date reminder and accepting my scheduled claim there, it is more likely that any September 23 interaction with the vendor originated inside the portal rather than from a stand-alone Sumsb email.

As detailed in Section II.B and Exhibit A, the acceptance email confirmed acceptance, gave no indication that KYC remained incomplete, and highlighted @kroll.com as the trusted domain. I had already completed Level-2 KYC directly with FTX US in 2021, and reasonably believed FTX already possessed my identification documents. That made the later Sumsb prompts—arriving from unfamiliar third-party domains—appear redundant and suspicious rather than authoritative. In that context, it was reasonable to believe the essential steps had been

completed through the official portal and to treat later non-@ftx.com / non-@kroll.com prompts with caution. To the extent the vendor logs show “initiation without final document upload,” that pattern is consistent with how a cautious user behaves when an unfamiliar third-party site, reached through multiple domains, requests highly sensitive identification information during a phishing-heavy period.

### 3. *Phishing studies show the Trust’s multi-domain KYC design made confusion foreseeable*

A substantial body of empirical research on phishing and security behavior shows that users rely heavily on sender and domain continuity to assess legitimacy, and that unfamiliar domains requesting sensitive data in a scam-heavy context routinely cause even well-intentioned users to halt or abandon the process. Studies such as *Dhamija, Tygar, and Hearst’s “Why Phishing Works” (CHI 2006)*<sup>6</sup> and later work by *Sheng, et al. (CHI 2010)*<sup>7</sup> and others document that domain mismatch and lack of clear, trusted indicators are among the strongest triggers for user suspicion and drop-off.

The KYC prompts I received contained no anti-phishing code, secret phrase, or other unique marker that I could verify against information inside the portal. According to a 2022 blog post by Sumsu<sup>8</sup> comparing major crypto exchanges, FTX did not offer an anti-phishing code, unlike some competitors. That design choice left domain continuity and sender recognition as the

<sup>6</sup> Rachna Dhamija, J. D. Tygar, and Marti Hearst. 2006. Why phishing works. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '06). Association for Computing Machinery, New York, NY, USA, 581–590. <https://doi.org/10.1145/1124772.1124861>

<sup>7</sup> Steve Sheng, Mandy Holbrook, Ponnurangam Kumaraguru, Lorrie Faith Cranor, and Julie Downs. 2010. Who falls for phish? a demographic analysis of phishing susceptibility and effectiveness of interventions. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10). Association for Computing Machinery, New York, NY, USA, 373–382. <https://doi.org/10.1145/1753326.1753383>

<sup>8</sup> Babar Ali. Oct 13, 2022. Who Has the Best Security Measures? Top 3 Crypto Exchanges Compared. In The Sumsu Blog. URL: <https://sumsub.com/media/spotlight/top-three-crypto-exchanges-compared/> (Accessed on November 18, 2025)

primary signals—precisely the areas where the KYC channel conflicted with the @ftx.com and @kroll.com guidance.

*4. Mixed fault, not casual disregard*

In hindsight, I should have contacted the claims agent or support directly to confirm whether my KYC verification was complete once I became unsure of my status. Failing to do that sooner was my mistake, and I acknowledge it. But that error did not arise in isolation.

The Debtors' process: (i) initiated verification through the official portal; (ii) sent an "Acceptance of Scheduled Claim" email that did not state that KYC remained incomplete; (iii) instructed customers to trust @kroll.com (and later @ftx.com) as authoritative domains; yet (iv) delivered highly sensitive KYC prompts from an unfamiliar and unexplained third-party sender and domain that did not match those trusted domains or identify the vendor in the body of the emails. Those messages bore objective hallmarks of phishing—unrecognized domain, no anti-phishing code, no vendor explanation, and passport-level document requests during a period of widespread crypto-related fraud. Put differently, the Trust and its vendors implemented a KYC workflow whose structure made lower completion rates among cautious users a foreseeable outcome, not an idiosyncratic reaction on my part.

My delay therefore reflects mixed fault: a fragmented, confusing security and communications design that made cautious non-completion more likely, combined with my own failure to resolve the uncertainty by reaching out sooner. It was not casual indifference to Court orders or deliberate disregard of clear warnings. This type of high-confusion, good-faith mistake by a retail creditor, where the only harm falls on the creditor, is consistent with circumstances courts have treated as excusable neglect under Rule 60(b)(1) of the Federal Rules of Civil Procedure.



And even if the Court finds it outside Rule 60(b)(1), the convergence of these factors is the kind of unusual, fact-specific situation that warrants narrowly tailored relief under Rule 60(b)(6).

#### **D. Good Faith**

There is no evidence, and the Trust does not contend, that I acted in bad faith.

- I accepted my scheduled claim and never tried to increase its amount.
- I did not seek any tactical advantage from delay; the only person placed at risk by my failure to complete KYC was myself.
- When the consequences of non-completion became clear, I moved promptly to address the issue through appropriate channels.

My conduct is consistent with that of a security-conscious retail customer navigating conflicting signals, not with someone trying to abuse the process.

### **V. RESPONSES TO SPECIFIC ARGUMENTS IN THE TRUST'S RESPONSE**

#### **1. "You started and abandoned KYC"**

The Trust's vendor logs reflect a KYC portal session on September 23, 2023 that was not completed. I do not have a precise memory of that session. What the logs cannot show is what happened after: I received an "Acceptance of Scheduled Claim" email that gave no warning of incomplete KYC and told me to trust @kroll.com. Combined with my prior Level-2 KYC with FTX US (which I reasonably believed was sufficient), that led me to think the process was done. The real confusion began with subsequent Sumsb emails that violated the domain guidance I had been given—a problem the logs don't capture.



## 2. “Self-created predicament”

The Trust’s “self-created predicament” label ignores that its own communications produced the core confusion. I followed an official Kroll reminder into the `claims.ftx.com` portal, accepted my scheduled claim, and received an acceptance email that said nothing about incomplete KYC while telling me to treat `@kroll.com` as the trusted domain; later, FTX Support instructed customers to “validate the sender’s domain is `@ftx.com` before proceeding.” By contrast, the KYC prompts that mattered most arrived as emails from an unfamiliar third-party sender, `no-reply@sumsub.com`, routing to `in.sumsub.com`, matching neither `@ftx.com` nor `@kroll.com` and offering no anti-phishing code, secret phrase, or clear in-email explanation of why that third-party vendor should be trusted with an identification document upload. Published phishing research shows that this type of combination—an unfamiliar third-party message from a mismatched domain seeking highly sensitive information without trusted indicators—predictably causes cautious users to halt or abandon the process. In that setting, my hesitation was a foreseeable reaction to conflicting signals, not disregard of clear instructions. Under Pioneer, the record reflects mixed fault, not a purely “self-created” problem.

## 3. “You ignored official resources”

The Trust’s claim that I “ignored” official resources such as the “Official Email Addresses” web page misstates what actually happened and shifts its own design burden onto a retail user. That page was a passive, static listing; it was never clearly incorporated into, or linked from, the Sumsub KYC emails themselves in a way that would reassure a cautious user receiving an unfamiliar, third-party request from an external sender and domain. No communication told me, in plain terms, that “`no-reply@sumsub.com` is our KYC vendor and you should trust

in.sumsub.com with your passport or driver's license," nor that this third-party address should override the @kroll.com guidance in my September 23, 2023 acceptance email or the later "validate @ftx.com" security rule. In short, I did not disregard a specific, targeted instruction; I failed to locate and cross-reference a stand-alone web page that the Debtors chose not to integrate into the actual high-risk KYC prompts they were sending.

#### 4. "Floodgates / precedent"

The Trust warns that granting relief here could open the floodgates to similar requests. But the Court retains full discretion to limit relief to this specific factual record: (i) I am a scheduled retail creditor whose claim amount is undisputed; (ii) I accepted my scheduled claim through the official portal; (iii) I had previously completed Level-2 KYC with FTX US before the bankruptcy; (iv) I began—but did not complete—the vendor's KYC flow at the identification-document step; (v) I received an acceptance email with no KYC warning and with @kroll.com domain guidance; (vi) I later received KYC prompts from a non-@ftx.com, non-@kroll.com domain that did not clearly explain the vendor relationship; and (vii) I acted promptly once I understood the consequence of non-completion. Nothing in this record compels relief for anyone else. Moreover, any future claimant seeking similar relief would still have to make an individualized evidentiary showing and undertake the same motion practice—including compiling email records, addressing the Trust's objections, and satisfying Pioneer—making this a natural filter that strongly undercuts any "floodgates" concern.

## VI. CONCLUSION

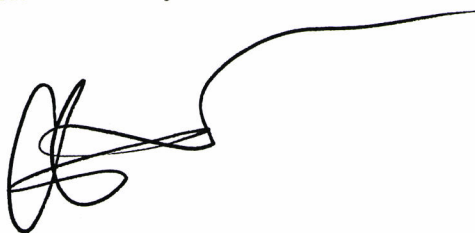
I am not asking the Court to unwind the KYC regime or reopen the bar date. I am asking the Court to recognize that, in this specific, email-driven, third-party KYC setup, a cautious user's error—shaped by portal-based initiation, an acceptance email silent on KYC, and conflicting domain guidance—combined with design-driven confusion to produce excusable neglect.

For the reasons set forth above, I respectfully request that the Court:

- Reconsider the expungement or disallowance of my claim under 11 U.S.C. § 502(j), Rule 60(b), and Rule 9006(b)(1);
- Restore my previously scheduled claim for the limited purpose of allowing me to complete KYC within a short period to be set by the Court (for example, 14 days); and
- Grant such other and further relief as the Court deems just and proper.

Dated: November 18, 2025

Redwood City, California

A handwritten signature in black ink, consisting of a series of loops and a long horizontal stroke extending to the right.

/s/ Daizhuo Chen

Daizhuo Chen (pro se)

1726 Maddux Dr, Redwood City, CA 94061

Phone: 646-286-8876

Email: chendaizhuo@gmail.com

## APPENDIX: EXHIBIT INDEX

- Ex. A-F. See the *Motion for Entry of an Order Authorizing Late Completion of Customer KYC* [D.I. 33349].
- Ex. G. Official FTX Noticing Email (September 22, 2023) from ftx@noticing.ra.kroll.com titled "Customer Claims Bar Date Reminder," used to access claims.ftx.com portal.
- Ex. H. Email from FTX Support (support@ftx.com, February 9, 2025) with banner instruction: "Please validate the sender's domain is @ftx.com before proceeding," which is difficult to reconcile with the Sumsb KYC channel (Exhibit D-2 through D-6).



Exhibit. G. Official FTX Noticing Email (September 22, 2023)  
from ftx@noticing.ra.kroll.com titled "Customer Claims Bar Date  
Reminder," used to access claims.ftx.com portal.



Henry Chen <chendaizhuo@gmail.com>

---

## In re FTX Trading Ltd. – Customer Claims Bar Date Reminder

---

Fri, Sep 22, 2023 at 9:00 PM

FTX Noticing <ftx@noticing.ra.kroll.com>  
Reply-To: ftxnoticing@kroll.com  
To: chendaizhuo@gmail.com

Dear Customer:

We would like to remind you that the **FTX Customer Claims Bar Date is September 29, 2023, 4 PM United States Eastern Time ("Bar Date")**. The Bar Date is the deadline to file proofs of claim, against the FTX Debtors, on account of Customer Claims. We recommend all customers with a customer claim to begin the claim process by logging in to the Customer Claims Portal at <https://claims.ftx.com>. If you have already filed a proof of claim and do not have any changes, then there is no need to file another claim.

Please note that the FTX Debtors have also requested KYC information as part of the customer claim process. As such, we urge you to begin the Know Your Customer ("KYC") process. Please note that it is **NOT** mandatory for you to have a verified KYC status in order to submit a claim. If you wish to submit a customer claim, you may do so during your KYC process prior to the Bar Date. Additionally, you do not need to have your KYC process completed and verified by the Bar Date. The KYC review and verification process will continue after the Bar Date.

Note that if your account was previously frozen as a result of the cybersecurity incident, please refer to the separate communication sent on September 17, 2023.

Please visit the FTX support website at <https://support.ftx.com> to learn more about the customer claim process and the KYC process. You may also contact our customer support team via email ([support@ftx.com](mailto:support@ftx.com)) if you have trouble logging in to the customer claims portal.

Sincerely,

FTX

FTX Noticing

Kroll Restructuring Administration LLC, 55 East 52nd Street, 17th Floor, New York, NY 10055

Unsubscribe

Exhibit. H. Email from FTX Support (support@ftx.com, February 9, 2023) with banner instruction: "Please validate the sender's domain is @ftx.com before proceeding," which is difficult to reconcile with the Sumsb KYC channel (Exhibit D-2 through D-6).

Henry Chen <chendaizhuo@gmail.com>

Sun, Feb 9, 2025 at 3:06 PM

FTX Customer Portal - Distribution Dashboard (Step 9) Now Live

FTX Support <support@ftx.com>  
To: chendaizhuo@gmail.com



**Please validate the sender's domain is @ftx.com before proceeding**  
FTX Recovery Trust will never ask you to connect your wallets

Dear Customer,

You are receiving this email in connection with the confirmed Second Amended Joint Chapter 11 Plan of Reorganization of FTX Trading Ltd. and its Debtor Affiliates [D.I. 26404-1] (the "Plan"), and Distributions you may be entitled to receive under the Plan.

The FTX Customer Portal has now released a Distribution Dashboard (Step 9). The Distribution Dashboard provides relevant information for your distribution including your selected Distribution Service Provider, estimated distribution date, and a breakdown of how your distribution amount was calculated.

For more information, please visit Distributions Dashboard FAQs.

Thank you,

FTX Customer Support

Note: If you suspect unauthorized access to your account, immediately lock your account, email support@ftx.com, and change your password.

IN THE UNITED STATES BANKRUPTCY COURT  
FOR THE DISTRICT OF DELAWARE

In re:  
FTX TRADING LTD., et al., Debtors.  
Chapter 11  
Case No. 22-11068 (JTD)  
(Jointly Administered)

**CERTIFICATE OF SERVICE**

I, Daizhuo Chen, certify that I am at least 18 years of age and that, on November 18, 2025, I served the *Reply in Further Support of Motion for Late KYC Completion (with exhibits)* upon:

**Sullivan & Cromwell LLP (Debtors/FTX Recovery Trust Counsel)**

- Andrew G. Dietderich — dietdericha@sullcrom.com — Means of Service: Email —  
Representing: Debtors/Trust
- James L. Bromley — bromleyj@sullcrom.com — Means of Service: Email —  
Representing: Debtors/Trust
- Brian D. Glueckstein — gluecksteinb@sullcrom.com — Means of Service: Email —  
Representing: Debtors/Trust
- Alexa J. Kranzley — kranzleya@sullcrom.com — Means of Service: Email —  
Representing: Debtors/Trust

**Landis Rath & Cobb LLP (Debtors' Delaware Counsel)**

- Adam G. Landis — landis@lrclaw.com — Means of Service: Email — Representing:  
Debtors/Trust
- Kimberly A. Brown — brown@lrclaw.com — Means of Service: Email — Representing:  
Debtors/Trust



- Matthew R. Pierce — pierce@lrclaw.com — Means of Service: Email — Representing: Debtors/Trust

**Paul Hastings LLP (Official Committee of Unsecured Creditors Counsel)**

- Kristopher M. Hansen — krishansen@paulhastings.com — Means of Service: Email — Representing: UCC
- Kenneth Pasquale — kenpasquale@paulhastings.com — Means of Service: Email — Representing: UCC
- Erez E. Gilad — erezgilad@paulhastings.com — Means of Service: Email — Representing: UCC
- Gabriele A. Sasson — gabesasson@paulhastings.com — Means of Service: Email — Representing: UCC
- Luc A. Despins — lucdespins@paulhastings.com — Means of Service: Email — Representing: UCC

**Young Conaway Stargatt & Taylor, LLP (Committee's Delaware Counsel)**

- Matthew B. Lunn — mlunn@ycst.com — Means of Service: Email — Representing: UCC
- Robert F. Poppiti, Jr. — rpoppiti@ycst.com — Means of Service: Email — Representing: UCC
- Joseph M. Kochenash — jkochenash@ycst.com — Means of Service: Email — Representing: UCC

**Office of the United States Trustee, Region 3**

- Linda Richenderfer — Linda.Richenderfer@usdoj.gov — Means of Service: Email —  
Representing: UST
- David Gerardi — David.Gerardi@usdoj.gov — Means of Service: Email —  
Representing: UST
- Benjamin A. Hackman — Benjamin.A.Hackman@usdoj.gov — Means of Service: Email  
— Representing: UST
- Jon Lipshie — Jon.Lipshie@usdoj.gov — Means of Service: Email — Representing:  
UST

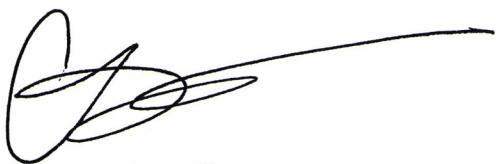
**Kroll Restructuring Administration LLC (Claims/Noticing Agent)**

- FTXInfo@ra.kroll.com — Means of Service: Email — Representing: Claims/Noticing
- ftxnoticing@ra.kroll.com — Means of Service: Email — Representing: Claims/Noticing
- FTXquestions@kroll.com — Means of Service: Email — Representing: Claims/Noticing

Additional Notice: All CM/ECF (Case Management / Electronic Case Files) registrants in Case No. 22-11068 (JTD) will receive notice via NEF (Notice of Electronic Filing) upon docketing by the Clerk.

Under penalty of perjury, I declare that the foregoing is true and correct.

Date: November 18, 2025

A handwritten signature in black ink, consisting of a large, stylized 'C' followed by a long horizontal stroke.

/s/ Daizhuo Chen

Daizhuo Chen

1726 Maddux Dr, Redwood City, CA 94061

Phone: 646-286-8876

Email: chendaizhuo@gmail.com



Insert shipping documents  
under window from the top.

Do not use this envelope for:

- UPS Ground
- UPS Standard
- UPS 3 Day Select®
- UPS Worldwide Expedited®



more than 100 years  
of Parcel Service.

International Shipping Notice - Carriage hereunder may be subject to the rules relating to liability and other terms and/or conditions established by the Convention for the Unification of Certain Rules Relating to International Carriage by Air (the "Warsaw Convention") and/or the Convention on the Contract for the International Carriage of Goods by Road (the "CMR Convention"). These commodities, technology or software were exported from the U.S. in accordance with the Export Administration Regulations. Diversion contrary to U.S. law prohibited.

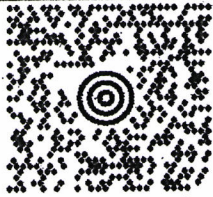
010195103

DAIZHUO CHEN  
6462868876  
1726 MADDUX DRIVE  
REDWOOD CITY CA 94061

1.0 LBS LTR

1 OF 1

SHIP TO:  
CLERK OF COURT  
DELAWARE U.S. BANKRUPTCY COURT  
824 N. MARKET STREET, 3RD FLOOR  
WILMINGTON DE 19801



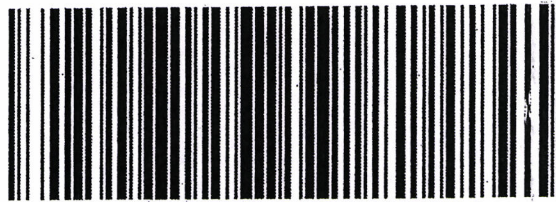
DE 197 9-25



UPS 2ND DAY AIR

TRACKING #: 1Z 628 21V 02 0629 1906

2



BILLING: P/P



XOL 25.10.09

NV45 47.0A 11/2025\*

The UPS Store RFID Label

Tracking #

1Z62821V020629 1906

Visit ups.com® or call 1-800-PICK-UPS® (1-800-742-5877)  
find a drop off location near you.

UPS Express Envelopes may only contain  
documents, and/or electronic media, and must  
contain envelopes containing items other than  
than 8 oz. will be billed by weight.

UPS Express Envelopes may only contain  
documents, and/or electronic media, and must  
contain envelopes containing items other than  
than 8 oz. will be billed by weight.

Wi  
Use t  
or ink